

ELECTRONIC PRIVACY INFORMATION CENTER

([Image files \(GIF\)](#) of this document are also available.)

Image Data, LLC

Identity Crime Prevention Pilot Program
Digitization Process Development Justification

To demonstrate that this technology can be deployed in states in which Department of Motor Vehicles databases are only partially (or not at all) digitized, Image Data will digitize a sample of the non-digitized driver's licenses in the State of Colorado database. By proving out this process we ensure the viability of deploying such service throughout the United States. We also, in the process, prove the viability to digitize the approximately three years worth of non-digitized licenses in the Colorado database. We thus cover the possibility that our pilot takes place in that state.

Image Data, LLC
Confidential

Image Data, LLC Proprietary

**Application of Identity Verification. and Privacy
Enhancement to Treasury Transactions, a Multiple Use
Identity Crime Prevention Pilot Project**

**Robert C. Houvener
Image Data, LLC
Nashua, NH**

**Submitted to:
U.S- Secret Service
Washington, DC 20223**

**April 1997
Updated November 1997**

Image Data, LLC Proprietary

1

Image Data, LLC Proprietary

1.0 Introduction

Identity based crimes cost U.S. local, state and federal governments, businesses and citizens many tens of billions of dollars as well as many injuries and deaths each year. When all ID based crimes and derivative crimes that depend upon false ID are taken into account it is likely that these entities are losing more than one hundred million dollars per day to this criminal activity. These crimes are perpetrated in areas such as checking, credit and debit cards, welfare and healthcare benefits, credit applications of all kinds, driver licenses and any other area in which it is of benefit for the criminal to assume another(s) identity. It is estimated that checking fraud alone, much of which is identity based, cost 12-15 billion dollars per year in the last few years. As with other forms of identity based crimes, check printing technology advancement is very much in favor of the criminal. Any fairly computer literate criminal can currently buy a computer, scanner and color printer and start scanning, modifying and printing their own checks. Driver licenses are counterfeited with similar but somewhat more sophisticated technology. In this age when an amateur counterfeiter can create his own, as well as forge others, documents this easily, a system is needed to verify that those presenting these documents for identification and payment purposes are truly who they say they are.

To date no system has been proposed that meets the significant demands of industry, the public and governmental bodies. The system and methods outlined in this document do address the requirements and concerns put forth. The concepts behind the system have been reviewed by leading industry and government entities charged with combating ID based crimes and they have universally expressed confidence that when implemented, it will solve a major portion of the ID based and derivative crimes in the U.S. After all the analysis, it is clear that this system will have

a greater impact on crime than any other single anticrime system in history. While achieving this, it will also do more to protect the privacy, public safety and identity of individuals than any financial transaction system enhancement in recent memory.

2.0 Objective

The U.S. government and the Treasury Department in particular send out billions of dollars per year to citizens and businesses. These payments reconcile obligation's such as retirement benefits of government employees, social services benefits, as well as other government obligations. As with other entities that are using checks and tokens such as magnetic stripe cards as a payment vehicle, the U.S. government is experiencing a significant and growing problem with fraud related to the payments it sends out. There is also a significant amount of fraud related to continuing to disperse benefits of deceased individuals. Due to the sheer magnitude of payments that the government sends out, this is a major loss to the citizens of the U.S. The responsibility for investigating crimes involving electronic transactions falls on the U.S. Secret Service. After meeting with leadership personnel in the Secret Service Financial Crimes Division, it became apparent that a joint pilot of the TrueID™ system in a defined geographical region of the U.S. would be of great benefit to the Treasury Department, Secret Service, citizens and

Image Data, LLC Proprietary

2

Image Data, LLC Proprietary

businesses of the U.S. The decision was made to move forward with a joint pilot project to demonstrate an effective means of combating the enormous and rapidly growing problem of identity based crime.

The objective of this pilot project will be to show the technical and financial feasibility of using remotely stored digital portrait images to securely perform positive identification of patrons putting forth financial instruments for negotiation or identity documents for access to services. At the same time, it will show how this can be accomplished in a cost effective manner while adding significant privacy enhancements in the transaction process for the individual patrons. This pilot project will use technology that has been developed in private industry. The pilot will demonstrate multiple use applications of the technology to commercial business transactions such as personal checks and in store credit cards, applications that can easily be extrapolated to government programs involving payment via EBT or paper checks. The federal government spends billions of dollars per year on law enforcement activities resulting from these crimes. The effort will be a joint private industry and federal government program and will include significant cooperative efforts from state governments in the pilots geographical area. The states have significant interest in this effort due the enormous amount of resources that they must apply in trying to combat these crimes at the state level.

A secondary but very important objective of the pilot will be to demonstrate how this technology can be used to prevent the issuance and use of counterfeit driver licenses at the state level, thereby cutting off the major source of false breeder documents. This pilot will be a model for future projects in showing how private industry, local, state and federal government entities can

cooperate to rapidly solve some of the major problems facing the U-S. today

3.0 Background

Current methods of identity verification actually compound the problem of identity based crimes. Efforts at identity verification such as printing name, address, phone number and writing driver license number or other personal identifiers on checks makes life easier for criminals. The use of the driver license as the ID of choice also makes it much easier for criminals to perform their acts. Not only is the driver license easily and regularly counterfeited, but official drivers license bureaus hand out hundreds of fake licenses per day due to an inability to detect that a person requesting a license has presented false documentation. These fake licenses are then used to perform numerous criminal acts which benefit from the assumption of a false identity.

Many companies have developed so called solutions to the problem of identity based crimes, but none of the. solutions has been adopted by the financial industry. The main reasons why these solutions have not been adopted is that they suffer from one of the following fatal drawbacks:

Image Data, LLC Proprietary

3

Image Data, LLC Proprietary

Too expensive

Too slow

Not usable in the mass market

Not acceptable by the public

No database of verification data available or easily developed

Not technically ready for widespread deployment

Not effective

Not compatible with current or emerging payment technologies

Some of the proposed systems to fight ID based crimes include technologies such as finger printing, retinal and iris scans, photo based cards and signature verification. All of these suffer from one or more of the fatal flaws noted above and have therefor not been generally adopted by industry.

Given all of the factors noted above, each of which must be overcome to provide an effective solution to the identity verification problem, one would expect that the solution would need to be very technically advanced and complex. This is not correct and a team of engineers at Image Data have developed a system that proves the old adage that the best ideas are sometime the simplest ideas. By combining knowledge and experience gained as a victim of credit card fraud with education and experience in engineering and high technology business management, Image Data's president invented a system which solves the vast majority of the identity based crime problem, while significantly enhancing privacy and addresses all of the critical factors noted above. This system, known as TrueID™, uses the same method that has been used for hundreds of years to identify individuals, the portrait photo. The difference between classic uses of the photo in the identity verification process and TrueID™ is that with TrueID™, the criminal

never gets access to the photo that is being used to verify their identity, This fusing of advanced technology with a tried and true method of positive identification yields a system that is highly effective, low cost and acceptable to the general public. This system can resolve many of the crimes that government, businesses and citizens are currently victimized by.

4.0 Technical Approach

The pilot will take place in a single state region. The portrait images will be acquired in digital format or as negatives from the Department of Motor Vehicles in the pilot state. The negatives will be digitized by Image Data. The digital images and corresponding identity information will then be processed and prepared for transmission over low speed Wide Area Network (WAN) communications lines. This processing includes sizing, color processing, compression and encryption of the data. The processing also includes loading the data into a real-time image retrieval database.

Remote retrieval devices will be manufactured and deployed at participating retail and financial institutions and the communications links between these institutions and Image

Image Data, LLC Proprietary

4

Image Data, LLC Proprietary

Data will be established. This includes interfacing the retrieval devices with the current point of use systems. Interfaces will also be set up with the Department of Motor Vehicles in the pilot states for database update purposes.

Finally, any necessary data will be collected from the participating financial institutions and loaded into the real-time retrieval system for image mapping purposes.

Upon commencement of the pilot, when a patron attempts a transaction at the participating institutions, their account number will be sent to Image Data and a digital image will be returned to the point of use in real-time. The image will then be used by the clerk to verify the identity of the patron. If an image is not available for that patron, the institution will revert to their old method of identity verification. If the account mapping is not in the Image Data database, a procedure will be followed to have it put into the database. This procedure applies equally to credit/debit card, EBT card or paper check transactions.

5.0 Pilot Project Tasks

Work with Secret Service to define list of proposed applications of the technology for the pilot.

Decide on applications to be piloted.

Define list of available states for pilots.

Map pilot applications to states.

Get buy-in and support of state entities to be involved in pilot.

If not on-line, acquire data, digitize and process images from state(s).

Define hardware, software and interface requirements for pilots.

Procure point of use devices for participating locations.
Choose institutions to participate in the pilot and get agreements in place.
Deploy devices at participating institutions.
Gather data from institutions for account mapping to images.
Test deployed system(s).
Go online and evaluate image delivery process.
Revise process as needed.
Go into pilot production mode and continue online pilot for 3 months.
Document results of pilot and report results.

6.0 Expected Results

Currently, U.S. state and federal governments spend over \$35 billion dollars per year fighting identity based crimes. Many more billions of dollars are lost directly by government due to it being the victim of these crimes. Finally, billions more dollars are lost in tax income due to businesses and individuals writing off against their profits their identity related losses on their tax returns, thereby significantly lowering tax income to the government. Due to technology advances that are easily accessible to the criminal, these figures are rapidly rising.

Image Data, LLC Proprietary

5

Image Data, LLC Proprietary

This program will demonstrate a highly effective way of reversing these losses and increasing tax revenue. The positive impact of this demonstration cannot be overstated. Once government agencies and businesses see the effectiveness of this technology and implement it for their own programs, the positive impact to state and federal budgets will be in the billions of dollars per year. There will also be significant public safety enhancements derived from this technology which will be measured by fewer deaths and injuries resulting from identity related crimes such as underage drinking, the rising use of identity crimes to finance illicit drug crimes and border jumping to obtain false driver licenses.

7.0 Deliverables

As a pilot project, the deliverables will consist of monthly progress reports, to be delivered by the end of the first full week of the month following the reporting period, as well as monthly briefings, to be delivered by the end of the second full week of the month following the reporting period, to the U.S. Secret Service. All monthly briefings will occur at U.S. Secret Service headquarters in Washington DC, except for:

- One briefing, approximately 8 weeks into the program, which will be a site visit by the USSS PM, at Image Data in Nashua, New Hampshire.
- One briefing at the pilot site by the USSS PM, prior to going live with the Pilot.
- One optional (at the USSS discretion) USSS PM site visit to the pilot site during the

operational phase of the pilot.

Image Data will be responsible for providing five copies of the status report and the briefing overhead presentation to the U.S. Secret Service Program Manager, with one copy to be sent directly to the U.S. Secret Service contracts representative.

The monthly status report will include:

- Detailed update on the status of each of the open tasks during the current reporting period.
- Reporting of any major issues that arose during the reporting period that could effect Image Data's ability to accomplish the tasks set forth for the pilot.
- A forward looking update on the tasks to be accomplished over the next two reporting periods and any major issues that are seen with these tasks, given the status of tasks during the present reporting period.
- Reporting on coordination efforts needed for site visits by USSS personnel.
- Reporting on key vendor activities.
- Reporting on relevant statistics that are generated during the reporting period and how these impact the pilot.
- Results of any specific statistical analysis requested by the USSS and agreed upon by Image Data at previous monthly briefings.

Image Data, LLC Proprietary

6

Image Data, LLC Proprietary

- Responses to any issues or questions raised during the last monthly status meeting.
- Details of any questions to be posed to the USSS that came up during the reporting period.

The oral briefing will review the data contained in the monthly written status report and will give the USSS the opportunity to engage Image Data in a question and answer session regarding the pilot project activities. The format of the written and oral reports will be reviewed after the delivery of the first report, in order to ensure that they are meeting the needs of the USSS.

8.0 Terms and Conditions

The following terms and conditions are the basis of this proposal:

- 1) The contract presented will be a firm fixed price contract.
- 2) All deliverables are as stipulated in paragraph 7.0 of this proposal.
- 3) The presumed start date of the contract will be December 15, 1997.
- 4) Payment terms are in accordance with the milestone payment schedule presented herein and payment will be made to Image Data thirty (30) days after receipt of invoice.
- 5) As marked in this proposal, all information provided is proprietary to Image Data, LLC, Nashua, NH.

9.0 Financial
See attached data.

Image Data, LLC Proprietary
7

[EPIC Privacy Page](#)